SISTEM PENDETEKSIAN PENYUSUPAN JARINGAN KOMPUTER DENGAN ACTIVE RESPONSE MENGGUNAKAN METODE HYBRID INTRUSION DETECTION, SIGNATURES DAN ANOMALY DETECTION

Novriyanto,ST., M.Sc [1], Haris Simare Mare, ST., MT [2], Wenni Syafitri [3]
[1]Teknik Informatika , Fakultas Science dan Teknologi, Universitas Islam Negeri Sultan Syarif Kasim Riau
Jl. HR. Soebrantas KM 15 Panam Pekanbaru – Riau
[2]Teknik Elektro , Fakultas Science dan Teknologi, Universitas Islam Negeri Sultan Syarif Kasim Riau
Jl. HR. Soebrantas KM 15 Panam Pekanbaru – Riau
[3]Teknik Informatika , Fakultas Science dan Teknologi, Universitas Islam Negeri Sultan Syarif Kasim Riau
Jl. HR. Soebrantas KM 15 Panam Pekanbaru - Riau
Email : [1]Novri_pci@yahoo.com, [2]harrismare@gmail.com, [3]Wenni20@gmail.com

ABSTRACT
The progress of internet technology increase the need of security data. The progress of tools which have intrusion ability, also influence these needed. The methods of Intrusion Detection System (IDS) implementation and methods of analyze intrusion have excess and lack, which mutually completes. There are a lot of IDS now, but just an IDS open source based is snort. Method of snort implementation is network based restricted. This Final Task's system used Hybrid Intrusion Detection System, Signatures and Anomaly Detection Methods. The indicator which used to detect intrusion are IP Address and Port Number. This system use TCP, UDP and ICMP protocols. This system also, is completed by active response, like blocking access for intruder. This System Implementation with Java Programming Language for engine perform and Java Server Pages (JSP) to develop user interface, The database which used is MYSQL. There are two of development test; Link system test and intrusion test. The link system test show the connect each interface. Intrusion is executed by host detection which used DoS HTTP tools and network detection which used Ping of Death's scripts. The intrusion testing conclusions are; can be detected, analyze and active response for intrusion.
.

Keywords : hybrid intrusion detection system, intrusion detection system (ids), signature and anomaly detection

1. PENDAHULUAN

Internet merupakan hal yang dibutuhkan pada zaman sekarang ini. Banyak aktivitas yang dapat dilakukan dengan media internet. Dari sekedar melakukan pencarian suatu artikel atau jurnal sampai kepada konsep berbelanja di dunia maya (*e-commerce*). Perkembangan ini memang sangat menguntungkan dan memudahkan pihak pemilik *website* untuk mempromosikan layanan atau fitur yang ditawarkan pada *client*. Begitu juga dari sisi *client*, kemudahan akses dengan hanya bermodalkan *pc* dan akses internet dapat menghilangkan keterbatasan akan ruang dan waktu.

Seiring kemajuan teknologi internet, ada sebuah kebutuhan yang mengikuti hal tersebut yaitu kebutuhan akan keamanan data pada *computer* yang sedang melakukan komunikasi melalui internet. Sebuah *computer* menjadi transparan atau mudah diakses dan beresiko untuk mengalami penyusupan dari pihak-pihak yang menginginkan untuk mengakses sistem komputer. Akibat ketransparan tersebut, sistem komputer secara langsung beresiko terhadap ancaman dan serangan. Hal ini sangat berbahaya bagi sistem komputer yang dimiliki sebuah korporasi atau perusahaan yang memiliki data-data yang sangat rahasia dan hanya boleh diakses oleh orang tertentu saja. Dapat kita bayangkan, dalam sekejap data tersebut bisa diakses dan dimanipulasi oleh pihak yang tidak memiliki hak akses. Bentuk lain dari ancaman yang sering terjadi yaitu pencurian terhadap data yang berharga dan rahasia, serta penyadapan terhadap data yang dikirim. Jika ruang lingkup *system* komputer hanya bersifat lokal, ancaman keamanan jaringan bisa terjadi dari 'orang dalam' yang berkeinginan untuk melakukan penyusupan dan melakukan ancaman terhadap sistem komputer. Dari hal-hal diatas, maka, dibutuhkan sebuah alat yang dikenal dengan nama *Intrusion Detection Systems (IDS)* atau *system* pendeteksi penyusupan.

Perkembangan metode dan *tool* penyusupan jaringan juga sangat mempengaruhi kebutuhan akan adanya sebuah *IDS* atau sistem pendeteksian penyusupan. Sehingga *IDS* dapat memberikan antisipasi dini terhadap resiko penyusupan. Ada berbagai jenis metode penyusupan misalnya *Denial of Service (DoS), Ping of Death, UDP Bomb* dan *tools* lainnya. Metode tersebut memiliki tujuan dalam menganggu proses kerja suatu *resource* atau jaringan sehingga tidak dapat bekerja sebagaimana mestinya.

Sebuah *Intrusion Detection System (IDS*) merupakan perangkat yang memiliki kemampuan untuk melakukan pendeteksian terhadap serangan dan ancaman yang terjadi pada sebuah jaringan komputer baik yang terhubung dengan internet

maupun hanya jaringan lokal. *IDS* memiliki peran yang sangat besar dalam mengamankan kerahasian suatu data dalam sebuah jaringan komputer.

Ada beberapa jenis *IDS* berdasarkan tempat dilakukannya implementasi *IDS*, yaitu *Host Intrusion Detection (HIDS) dan Network Intrusion Detection System (NIDS)*. Kedua jenis *IDS* diatas juga memiliki kelebihan dan kekurangan yang apabila diintegrasikan maka akan memperkecil kekurangan dan menguatkan kelebihan yang dimiliki masing-masing tipe. Salah satu kelebihan *NIDS* yaitu dapat mendeteksi serangan yang tidak terdeteksi oleh *HIDS*. Begitu juga sebaliknya dengan *HIDS*. Kekurangan dari *NIDS* yaitu keterbatasan dalam me-*monitoring host* secara lebih detail, sedangkan *HIDS* tidak mampu melakukan *monitoring traffic* secara keseluruhan.

Dalam melakukan pendeteksian sebuah *IDS* menggunakan dua metode *Signatures* dan *Anomaly Detection. Signatures* merupakan pembandingan antara *rules* atau aturan antara sebuah *traffic* yang sedang dideteksi dengan *traffic* yang mengidentifikasikan terjadinya penyerangan. Sedangkan *Anomaly* ialah perbandingan antara *rules* yang berisi *traffic* normal dengan *traffic* yang sedang dideteksi. *Signature*s memiliki kelemahan dalam menidentifikasi serangan yang tidak didefinisikan pada *rules* yang berisi informasi ciri-ciri penyerangan, sehingga IDS yang menggunakan metode *signatures* tidak mengenali penyerangan baru yang belum terdapat pada *rules*. Jika ditinjau pada metode *Anomaly*, maka pendeteksi pun bisa dimanipulasi agar bisa mendeteksi serangan yang belum terdapat pada *rules Signatures*.

Telah banyak *Intrusion Detection System* yang berkembang disaat ini, yaitu *RealSecure* dari *Internet Security Systems (ISS), Cisco Secure Intrusion Detection System* dari *Cisco Systems* (yang mengakuisisi *WheelGroup* yang memiliki produk *NetRanger*), *eTrust Intrusion Detection* dari *Computer Associates* (yang mengakusisi MEMCO yang memiliki *SessionWall-3*), *Symantec Client Security* dari *Symantec, Computer Misuse Detection System* dari *ODS Networks, Kane Security Monitor* dari *Security Dynamics, Cybersafe, Network Associates, Network Flight Recorder, Intellitactics, SecureWorks, Snort, Security Wizards, Enterasys Networks, Intrusion.com, IntruVert, ISS, Lancope, NFR, OneSecure, Recourse Technologies*, dan *Vsecure.*

Namun ada sebuah *IDS* yang berbasiskan *open source* yaitu *Snort*. *Snort* hanya memanfaatkan konsep pendeteksian yang berdasarkan *Network-based* yang hanya melakukan penganalisaan terhadap paket data yang dianggap sebagai serangan yang melintasi *network*. Sedangkan pendeteksian secara *host*-based yang dikenal dengan nama *Host Intrusion Detection System (HIDS)* merupakan hal yang penting dilakukan agar keamanan *host* tempat *resources* memiliki faktor keamanan. Berdasarkan jenis metode analisa *rules* yang dikategorikan sebagai penyusupan, *Snort* menggunakan metode analisa *signatures* dan *anomaly detection.*

Berdasarkan latar belakang diatas, maka dirancanglah sebuah *IDS* yang berbasiskan *Hybrid Detection System, Signatures dan Anomaly Detection*.

2. TUJUAN PENELITIAN

Tujuan penelitian ini adalah membangun sebuah *IDS* yang mampu mengamankan secara aktif, *traffic* jaringan dan *host* dari resiko penyusupan dengan mengintegrasikan konsep *Hybrid Detection System, Signatures* dan *Anomaly detection* secara optimal.

3. BATASAN MASALAH

Untuk menghindari salah pengertian dalam penulisan Batasan masalah dari penyusunan tugas akhir ini adalah :

a) Protokol yang digunakan yaitu *TCP*, *UDP*, dan *ICMP*
b) Fitur yang dimiliki oleh sistem ini difokuskan kepada tiga bagian, sebagai berikut :
    a. *Sniffer mode*, untuk melihat paket lewat di *network*
    b. Paket *Logger mode*, untuk mencatat semua paket yang lewat di *network* dan akan dilakukan penganalisaan di masa mendatang
    c. *HyDManSys Mode* yang terdiri atas dua sub bagian:
        i. *Network Intrusion detection mode*, berfungsi untuk mendeteksi serangan yang melalui jaringan
        ii. *Host Intrusion detection mode*, berfungsi untuk mendeteksi serangan yang terjadi pada suatu *host*
c) Indikator yang digunakan dalam analisa penyusupan jaringan ialah *Internet Protokol Address (IP Address)* dan *port number*

4. LANDASAN TEORI

4.1 Penyusupan Jaringan

Penyusupan Jaringan merupakan suatu pengaksesan yang dilakukan seseorang atau komputer yang tidak memiliki hak otorisasi terhadap sumber daya yang akan diakses. Ada berbagai tipe penyusupan yang terjadi pada jaringan, sebagai berikut (Berbagai,2008):

1. *LAND Attack*

Adalah salah satu macam serangan terhadap suatu server yang terhubung dalam suatu jaringan untuk menghentikan layanan, sehingga terjadi gangguan terhadap layanan atau jaringan komputer.

2. *Ping of Death*

Ping of Death merupakan suatu serangan (*Denial of Service) DoS* yang memanfaatkan fitur yang ada di *TCP/IP* yaitu *packet fragmentation* atau pemecahan paket.

3. *Teardrop*

Teardrop attack adalah suatu serangan bertipe *Denial of Service (DoS)* terhadap suatu *server* atau komputer yang memanfaatkan fitur yang ada di *TCP/IP* yaitu *packet fragmentation* atau pemecahan paket, dan kelemahan yang ada di *TCP/IP* pada waktu paket-paket yang terfragmentasi tersebut disatukan kembali.

4. *Half-Open Connection*

Dalam serangan *half-open connection*, penyerang mengirimkan ke server yang hendak diserang banyak paket *SYN* yang telah di-*spoof* atau direkayasa sehingga alamat asal (*source address)* menjadi tidak valid.

5. *UDP Bomb Attack*

Untuk melakukan serangan *UDP Bomb* terhadap suatu *server*, seorang penyerang mengirim sebuah paket *UDP (User Datagram Protocol)* yang telah di-*spoof* atau direkayasa sehingga berisikan nilai-nilai yang tidak *valid* di *field* tertentu.

4.2 Definisi Sistem Pendeteksian Penyusupan

Sistem Pendeteksian Penyusupan, lebih dikenal dengan nama *IDS (Intrusion Detection System)*. Sistem ini merupakan usaha mengidentifikasi adanya penyusup yang memasuki sistem tanpa otorisasi (misal *cracker*) atau seorang user yang sah tetapi menyalahgunakan *privilege* sumberdaya sistem.

4.3 Protokol-Protokol Tang Digunakan pada Penelitian

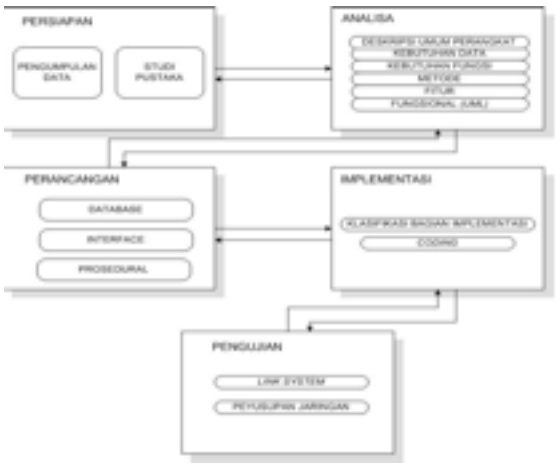
Protokol merupakan media antar perangkat *(devices)* dalam berkomunikasi. Apabila akan dilakukan pertukaran informasi antar beberapa komputer dalam suatu jaringan, maka protokol-lah yang menjadi media komunikasi. Ada berbagai jenis protokol, namun pada penelitian ini akan difokuskan kepada protokol *TCP*, *UDP*, dan *ICMP*..

4.4 Java Runtime Environment

Java Runtime Environment, (JRE) merupakan sebuah perangkat lunak yang dibutuhkan untuk menjalankan semua aplikasi yang berbasis *Java Platform*. JRE banyak sekali digunakan sebagai *plug-ins web browser* dan dalam berbagai program kontemporer. *Sun Microsystem* juga meluncurkan *superset* dari *JRE* dan diberi nama *Java 2 SDK*, yang sering disebut *JDK*. Dalam *JDK* ini terdapat beberapa komponen pengembangan *Java*, seperti : *Java Compiler*, *Javadoc*, *Jar* dan *debugger*.

5. METODOLOGI PENELITIAN

Tahapan Penelitian yang akan dilaksanakan pada pengembangan sistem penyusupan Jaringan Komputer ini dapat terlihat pada gambar 1 dibawah ini:



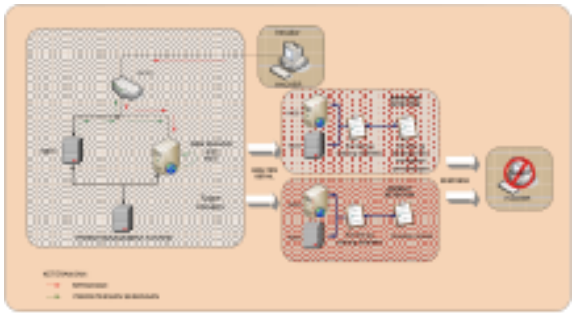
Gambar 1. Tahapan Penelitian

6. ANALISA DAN PERANCANGAN SISTEM

6.1 Deskripsi Umum Perangkat Lunak

Deskripsi umum merupakan pengambaran umum unjuk kerja atau perangkat lunak yang akan dibangun. Perangkat lunak yang akan dibangun adalah perangkat lunak yang memiliki kemampuan untuk pendeteksian terhadap penyusupan pada jaringan komputer baik secara pendekatan *host* maupun *network*. Perangkat ini juga memiliki kemampuan untuk menganalisa dengan metode *signature* dan *anomaly detection*.

Berikut penggambaran umum dari perangkat lunak yang akan dibangun pada gambar 2



Gambar 2 Deskripsi Umum Perangkat Lunak

Rincian penjelasan deskripsi umum perangkat lunak, dapat dilihat pada uraian dibawah ini, sebagai berikut :

1. *Intruder* (Penyusup), melakukan penyusupan pada target operasi dengan sasaran utama yaitu *Web Server* yang dimiliki sebuah *network*
2. *Hybrid IDS Management System (HyIDS ManSys)* merupakan sistem utama yang memegang kendali terhadap keamanan *traffic network*. *HyIDS ManSys* memiliki beberapa tugas, yaitu:

a. Menyimpan data kondisi *signature* dan *anomaly*
b. Melakukan pendeteksian secara *real time* pada *resource host (Web Server)* dan *traffic* jaringan
c. Menganalisa kondisi *traffic* jaringan dan *host* baik secara *signature* dan *anomaly detection*
d. Memberikan peringatan (*alert*) terhadap kondisi yang dikategorikan sebagai penyusupan
e. Melakukan *response* berupa *access blocking* terhadap penyusupan yang dilakukan *Intruder*

6.2 Analisa Perangkat Lunak

Analisa Perangkat Lunak bermanfaat sebagai penentu proses pengerjaan agar ditemukannya suatu pemecahan masalah. Terciptanya keruntunan suatu analisa perangkat lunak pada jalur yang benar merupakan dasar dilakukannya tahap ini.

6.2.1 Analisa Kebutuhan Data

Analisa Analisa kebutuhan data yang terdapat pada perangkat lunak ini, ialah :

1. Inisialisai data awal perangkat lunak berdasarkan metode yang digunakan, terbagi atas dua hal, sebagai berikut :
   a. *Signature* Data, berisi data yang dikategorikan sebagai penyusupan pada *host* dan *traffic* jaringan. Berdasarkan metode yang digunakan data ini dapat berupa;
      i. *Host* memiliki data berupa *ip address host*, *ip address* yang berhak untuk mengakses *host*, *event* yang dilakukan *host*
      ii. *Traffic* memiliki data berupa *ip address* tujuan, *ip address* asal, *port*, protokol
   b. Data *Anomaly* berisi data kondisi normal suatu *host* dan *traffic* jaringan. Detail data memiliki kesamaan dengan Data *signature*.
2. Menangkap (*capture*) atau proses *sniffer* terhadap data kondisi pada resource *host* dan *traffic* jaringan, ketika dilakukan pengaktifan *HyIDS ManSys* baik pada *host* maupun *traffic* dan keduanya secara bersamaan. Secara umum, pencatatan juga dilakukan pada data tanggal dan kondisi proses *sniffer*. Berikut penjelasan lebih lanjut mengenai proses *sniffer* berdasarkan data kondisi pada *host* dan *traffic* yaitu :
   a. *Host* memiliki data berupa *ip address host*, *ip address* yang berhak untuk mengakses *host*, *event* yang dilakukan *host*
   b. *Traffic* memiliki data berupa *ip address* tujuan, *ip address* asal, *port*, protokol

6.2.2 Analisa Kebutuhan Fungsi

Analisa Perangkat lunak ini memiliki beberapa fungsi yang bisa dimanfaatkan oleh user agar dapat menghasilkan output yang maksimal dan berjalan sebagaimana mestinya. Berikut rincian analisa kebutuhan fungsi bagi user, yaitu :

1. Fungsi aktivasi *Network Intrusion Detection* dan *Host Intrusion Detection*
2. Fungsi input *network signature* dan *host signature*
3. Fungsi *capture* kondisi normal yang berguna dalam proses analisa *Anomaly Detection*
4. Fungsi Sniffing atau proses penangkapan kondisi *Host* dan *Network*
5. Fungsi proses analisa secara *signature* dan *anomaly detection* baik pada *host* dan *network*
6. Fungsi penyimpanan *alert* atau peringatan dan *response*

6.2.3 Analisa Metode yang akan digunakan pada Perangkat Lunak

Analisa metode yang dilakukan oleh *Hybrid Intrusion Detection Management System* meliputi dua bagian, sebagai berikut :

1. *Host Intrusion Detection System (HIDS)*, pada bagian ini terdapat dua metode pendeteksian yang akan dilakukan, yaitu :
   a. *Signature Detection*, merupakan proses penganalisaan suatu kondisi *host* dengan membandingkan kondisi yang sedang dideteksi dengan *signature rules* yang telah diinputkan sebelumnya. *Signature rules* berisi *rules* yang dikategorikan sebagai penyusupan.
   b. *Anomaly detection* ialah proses penganalisaan suatu kondisi *host* dengan membandingkan kondisi normal *host* dengan kondisi yang sedang terdeteksi, selanjutnya akan dikategorikan sebagai penyusupan apabila terjadi perbedaan dari kedua kondisi.

2. *Network Intrusion Detection System (NIDS)*, pada bagian ini terdapat dua metode yang akan dilaksanakan, yaitu :
   a. *Signature Detection*, merupakan proses penganalisaan suatu kondisi *traffic* dengan membandingkan kondisi yang sedang dideteksi dengan *signature rules* yang telah diinputkan sebelumnya. *Signature rules* berisi *rules* yang dikategorikan sebagai penyusupan.
   b. *Anomaly detection* ialah proses penganalisaan suatu kondisi *traffic* dengan membandingkan kondisi normal *traffic* dengan kondisi yang sedang terdeteksi, selanjutnya akan dikategorikan sebagai penyusupan apabila terjadi perbedaan dari kedua kondisi

6.2.4 Analisa Fitur yang akan dibangun pada Perangkat Lunak

Fitur yang dikembangkan pada perngkat lunak ini, ialah :

a. *Sniffer mode*, untuk melihat paket lewat di *network*
b. Paket *Logger mode*, untuk mencatat semua paket yang lewat di *network* dan akan dilakukan penganalisaan di masa mendatang
c. *Network Intrusion Detection mode*, berfungsi untuk mendeteksi serangan yang melalui jaringan
d. *Host Intrusion Detection mode*, berfungsi untuk mendsteksi serangan yang terjadi pada suatu *host*

6.2.5 Analisa Fungsional

Analisa fungsional yang digunakan didasari pada *Unified Managed language (UML)*. Analisa fungsional ini terdari pembahasan *Use Case Diagram*, *Class Diagram* dan *Deployment Diagram*. *Gambar 3 dibawah ini menunjukan Use Case Diagram* dari perangkat lunak.

Gambar 3 *Use Case Diagram*

6.3 Perancangan Perangkat Lunak

Perancangan ialah tahap yang dilaksanakan setelah dilakukan analisa pada perangkat lunak. Perancangan ini berguna agar proses implementasi yang dilakukan dapat konsisten dan sesuai dengan analisa yang dilakukan. Perancangan yang dilakukan meliputi perancangan *database*, struktur menu dan tampilan.

6.3.1 Perancangan Database

Database merupakan bagian yang sangat berperan penting dalam perangkat ini. Di dalam database lah disimpan *rules* yang berkaitan dengan unjuk kerja dari *Hybrid IDS* ini, serta penyimpanan hasil-hasil kegiatan dalam pendeteksian penyusupan jaringan, seperti kondisi pendeteksian, *management alert* dan *management response*.

Perancangan *Database* yang dilaksanakan pada perangkat lunak ini berdasarkan tabel data yang digunakan. Ada sembilan tabel yang terdapat pada perangkat lunak ini, yaitu *User*, *SignatureNIDS*, *SignatureHIDS*, *KondisiNormalHIDS*, *KondisiNormalNIDS*, *Alert*, *Respon*, *KondisiPendeteksianHost*, *KondisiPendeteksianNids.*

6.3.2 Perancangan Tampilan Sistem

Perancangan terhadap tampilan yang akan dibangun merupakan hal yang sangat penting dalam terciptanya kekonsistenan implementasi. Perancangan tampilan ini terdiri atas dua bagian yaitu struktur menu dan *interface*.

6.3.3 Perancangan Prosedural

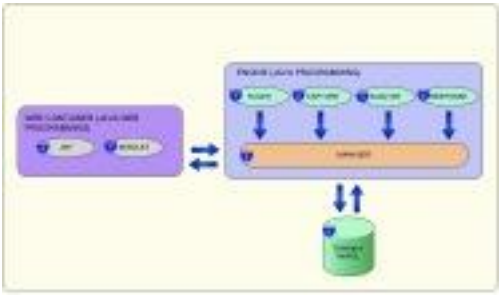
Perancangan prosedural yang dilaksanakan pada pengembangan perangkat lunak ini dapat terlihat *pseudo code* algoritma unjuk kerja utama untuk melakukan proses pendeteksian penyusupan.

7. IMPLEMENTASI DAN PENGUJIAN

7.1 Implementasi Perangkat

Tahapan implementasi ialah tahapan yang dicapai ketika perangkat telah selesai untuk digunakan dan bermanfaat untuk melihat ketercapaian sistem yang dibangun sesuai dengan tujuan pembangunan sistem. Tahapan ini terdiri dari proses penulisan program, uji sub sistem dan penggabungan sistem.

Implementasi perangkat seperti terlihat pada gambar 4 dibawah ini, menggunakan bahasa pemograman *Java* dan *Java Server Pages (JSP)* serta database *MySQL*.



Gambar 4 Implementasi Perangkat

Pada proses implementasi terdapat tiga bagian utama dalam pengembangan perangkat ini. Berikut deskripsi implementasi perangkat yang telah dilaksanakan, yaitu:

a. Implementasi *Engine*, ialah tahapan inti dari pengembangan perangkat. pada tahap ini terdapat beberapa sub bagian, sebagai berikut:
   1) *Rules* merupakan implementasi dari *class* data-data inputan, misalnya : *Signature Host*, *Signature Network*,

Kondisi Normal *Host* dan Kondisi Normal *Network*

2) *Capture* ialah implementasi data yang dihasilkan ketika proses *capture* (penangkapan) kondisi *network* dan *host*.
3) *Analyze* adalah implementasi dari data proses pendeteksian terhadap penyerangan
4) *Response* merupakan implementasi data respon yang telah dilakukan terhadap penyerangan
5) *Manager* ialah penghubung antara *class rules*, *capture*, *analyze* dan *response* dengan pemrograman berbasiskan *web*, serta berperan dalam pengaturan method-method yang akan dieksekusi terhadap *class.*

b. Implementasi Berbasiskan *web*

1) *Servlet* adalah penghubung dinamis antara *web server* dengan *user*. Atau disebut sebagai penghubung tampilan *Java Server Pages* dengan *web server*. *Servlet* berjalan disisi *server.*
2) *Java Server Pages (JSP)* merupakan halaman web yang berisi tampilan yang dapat dilihat secara kasat mata oleh *user*. Setiap eksekusi yang akan dilakukan pada perangkat oleh *user*, selalu dimulai dengan interaksi dengan halaman *JSP* ini

c. Implementasi *Database*

Database yang digunakan ialah *MySQL*

7.2 Pengujian Sistem

Pengujian Setelah tahapan implementasi selesai dilaksanakan, tahap selanjutnya yaitu pengujian perangkat. Identifikasi dan rencana pengujian dapat dilihat pada Tabel 1 berikut ini

Tabel 1. Pengujian Sistem

Kelas Uji	Butir Uji	Tingkat Pengujian	Jenis Pengujian
Link dalam sistem	Normal	Pengujian sistem HydManSys	*Black box*
Percobaan penyusupan jaringan	Normal	Pengujian sistem HyDManSys	*Black box*

8. KESIMPULAN DAN SARAN

8.1 Kesimpulan

Kesimpulan yang didapat pada pengembangan perangkat yang telah dilaksanakan, ialah *Hybrid Intrusion Detection Management System (HyDManSys)* dapat melakukan *capture*, analisa dan respon (*blocking access*) pada penyusupan jaringan sehingga berperan aktif dalam pendeteksian, dengan mengintegrasikan metode *Hybrid Intrusion Detection System, Signatures* dan *Anomaly Detection.* Namun, pada pengembangan perangkat ini, memiliki kekurangan dalam pendeteksian penyusupan, yang disebabkan oleh pembatasan masalah tugas akhir ini yaitu pada indikator dan protokol yang digunakan untuk mendeteksi penyusupan.

8.2 Saran

Berdasarkan kesimpulan yang telah dipaparkan sebelumnya, saran untuk pengembangan perangkat selanjutnya, ialah :

Penggunaan protokol yang tidak hanya terbatas pada protokol *TCP*, *UDP* dan *ICMP* misalnya penggunaan protokol *SNMP (Simple Network Monitoring Protokol)*

Indikator yang digunakan dalam analisa penyusupan jaringan tidak hanya terbatas pada indikator *IP Address* dan *Port.*

PUSTAKA

Ariyus, Dony.(2007). "*Sistem Pendeteksian Penyusupan"*.Yogyakarta, Andi, 2007

_____.(2010). "*Berbagai Macam Serangan Terhadap Jaringan Komputer".* Diakses 6 Januari 2010. dari http://www.konche.org/details. php?id=49,

_____,(2009*) "Jaringan".* Diakses 3 April 2010. dari http://www.virologi.info/modul/ Jaringan.pdf

_____, (2009*). "Java"*. Diakses 10 Maret 2009 dari http://www.ittelkom.ac.id/ library/index.php?view=article&catid=6%3Ainternet&id=32%3Ajava&option=com_content&Itemid=15,

Setiawan, Deris. (2009) "*Bab 2 TCP/IP"*. diakses 3 April 2009 dari http://ilkom.unsri.ac.id/dfiles/materi/jarkom/ bab2 -TCPIP.pdf,